AMENDMENTS TO THE CLAIMS

Please cancel claims 1-26.

Please amend claim 27 as follows:

27. (Currently Amended) An apparatus, comprising:

means for establishing, in an operating system environment controlled by a single operating system kernel instance, a global zone and at least ~~one~~ a first non-global zone for isolating processes in the first non-global zone from processes in other non-global zones ~~in an operating system environment controlled by a single operating system kernel instance~~;

means for receiving, from a first process executing in association with the first non-global zone, a first request to perform ~~an~~ a first operation;

means for determining in response to ~~receiving~~ the first request whether performing the ~~requested~~ first operation enables the first process to obtain additional privileges for which the first process is not authorized; and

means for denying the first request if performing the first operation enables the first process ~~is enabled~~ to obtain ~~the~~ additional privileges for which the first process is not authorized.

Please add the following new claims:

28. (New) A method, comprising:

in an operating system environment controlled by a single operating system kernel instance, establishing a global zone and at least a first non-global zone for isolating processes in the first non-global zone from processes in other non-global zones;

receiving, from a first process executing in association with the first non-global zone, a first request to perform a first operation;

in response to the first request, determining whether performing the first operation enables the first process to obtain additional privileges for which the first process is not authorized; and

denying the first request if performing the first operation enables the first process to obtain additional privileges for which the first process is not authorized.

29. (New) The method of claim 28, wherein each non-global zone has a set of allowable privileges for processes executing within the non-global zone.

30. (New) The method of claim 29, wherein the first operation comprises obtaining control of a second process, wherein the first process has a first set of process privileges, wherein the second process has a second set of process privileges, and wherein determining whether performing the first operation enables the first process to obtain additional privileges for which the first process is not authorized comprises:

determining if a zone identifier of the first process matches a zone identifier of the second process;

if the zone identifiers do not match:

determining if the first process is associated with a non-global zone; and if so, concluding that performing the first operation enables the first process to obtain additional privileges for which the first process is not authorized;

if the first process is not associated with a non-global zone, determining if the first process has a privilege to control processes in other zones; and if the first process does not have the privilege to control processes in other zones, concluding that performing the first operation enables the first process to obtain additional privileges for which the first process is not authorized;

determining if a user identifier of the first process matches a user identifier of the second process;

if the user identifiers do not match, determining if the first process has a privilege to take control of processes belonging to other user identifiers; and if the first process does not have the privilege to take control of processes belonging to other user identifiers, concluding that performing the first operation enables the first process to obtain additional privileges for which the first process is not authorized;

determining if the first set of process privileges includes every privilege in the second set of process privileges; and if the first set of process privileges does not include every privilege in the second set of process privileges, concluding that performing the first operation enables the first process to obtain additional privileges for which the first process is not authorized.

31. (New) The method of claim 30, wherein the first non-global zone has a first set of allowable privileges, and wherein the method further comprises:

determining if the user identifier of the second process is a privileged user identifier;

if the user identifier of the second process is not a privileged user identifier, concluding that performing the first operation does not enable the first process to obtain additional privileges for which the first process is not authorized; thus, the first request is granted;

if the user identifier of the second process is a privileged user identifier, determining if the first process is associated with the global zone;

if the first process is associated with the global zone, determining if the first process has all global zone privileges; and if not, concluding that performing the first operation enables the first process to obtain additional privileges for which the first process is not authorized;

if the first process is not associated with the global zone, determining if the first process has all of the privileges in the first set of allowable privileges; and if not, concluding that performing the first operation enables the first process to obtain additional privileges for which the first process is not authorized.

32. (New) The method of claim 29, wherein establishing the first non-global zone for isolating processes in the first non-global zone from processes in other non-global zones, comprises:

setting a privilege limit for the first non-global zone, the privilege limit indicating the set of allowable privileges for processes executing within the first non-global zone.

33. (New) The method of claim 32, wherein the privilege limit is represented as a bit mask passed to the first non-global zone when the first non-global zone is created, the method further comprising:

comparing privileges held by a process joining the first non-global zone against the bit mask; and removing any privileges not in the bit mask from the process joining the first non-global zone.

34. (New) The method of claim 28, wherein performing the first operation comprises accessing an object, the method further comprising:

determining whether the first process has permission to access the object.

35. (New) The method of claim 28, wherein the first operation includes one of: mounting/unmounting a file system, overriding file system permissions, binding to a privileged network port, and controlling other processes with different user identifiers.

36. (New) The method of claim 29, wherein the first operation comprises changing a user identifier associated with the first process, wherein the first non-global zone has a first set of allowable privileges, and wherein determining whether performing the first operation enables the first process to obtain additional privileges for which the first process is not authorized comprises:

determining if the first operation is changing the user identifier associated with the first process to a privileged user identifier;

if the first operation is not changing the user identifier associated with the first process to a privileged user identifier, determining if the first process has a privilege to set its own user identifier; and if not, concluding that performing the first operation enables the first process to obtain additional privileges for which the first process is not authorized;

if the first operation is changing the user identifier associated with the first process to a privileged user identifier, determining whether the first process has all of the privileges in the first set of allowable privileges, and if not, concluding that performing the first operation enables the first process to obtain additional privileges for which the first process is not authorized.

37. (New) The method of claim 28, further comprising:

receiving, from a second process executing in association with the global zone, a second request to perform a second operation;

in response to the second request, determining whether performing the second operation enables the second process to obtain additional privileges for which the second process is not authorized; and

denying the second request if performing the second operation enables the second process to obtain additional privileges for which the second process is not authorized.

38. (New) The method of claim 37, wherein the second operation comprises obtaining control of a third process, wherein the second process has a first set of process privileges, wherein the third process has a second set of process privileges, and wherein determining whether performing the second operation enables the second process to obtain additional privileges for which the second process is not authorized comprises:

determining if a zone identifier of the second process matches a zone identifier of the third process;

if the zone identifiers do not match:

determining if the second process is associated with a non-global zone; and if so, concluding that performing the second operation enables the second process to obtain additional privileges for which the second process is not authorized;

if the second process is not associated with a non-global zone, determining if the second process has a privilege to control processes in other zones; and if the second process does not have the privilege to control processes in other zones, concluding that performing the

second operation enables the second process to obtain additional privileges for which the second process is not authorized;

determining if a user identifier of the second process matches a user identifier of the third process;

if the user identifiers do not match, determining if the second process has a privilege to take control of processes belonging to other user identifiers; and if the second process does not have the privilege to take control of processes belonging to other user identifiers, concluding that performing the second operation enables the second process to obtain additional privileges for which the second process is not authorized;

determining if the first set of process privileges includes every privilege in the second set of process privileges; and if the first set of process privileges does not include every privilege in the second set of process privileges, concluding that performing the second operation enables the second process to obtain additional privileges for which the second process is not authorized;

determining if the user identifier of the third process is a privileged user identifier;

if the user identifier of the third process is not a privileged user identifier, concluding that performing the second operation does not enable the second process to obtain additional privileges for which the second process is not authorized; thus, the second request is granted;

if the user identifier of the third process is a privileged user identifier, determining if the second process is associated with the global zone; and

if the second process is associated with the global zone, determining if the second process has all global zone privileges; and if not, concluding that performing the second operation

enables the second process to obtain additional privileges for which the second process is not authorized.

39. (New) The method of claim 37, wherein the second operation comprises changing a user identifier associated with the second process, and wherein determining whether performing the second operation enables the second process to obtain additional privileges for which the second process is not authorized comprises:

determining if the second operation is changing the user identifier associated with the second process to a privileged user identifier;

if the second operation is not changing the user identifier associated with the second process to a privileged user identifier, determining if the second process has a privilege to set its own user identifier; and if not, concluding that performing the second operation enables the second process to obtain additional privileges for which the second process is not authorized;

if the second operation is changing the user identifier associated with the second process to a privileged user identifier, determining whether the second process has all global zone privileges, and if not, concluding that performing the second operation enables the second process to obtain additional privileges for which the second process is not authorized.

40. (New) The method of claim 37, wherein the second operation includes one of: modifying all process privileges, writing to system administration file, opening device holding kernel memory, modifying operating system code, accessing file systems restricted to root user, setting the system clock, changing scheduling priority of an executing process,

reserving resources for an application, directly accessing a network layer and loading kernel modules.

41. (New) A computer readable medium comprising a set of one or more instructions which, when executed by one or more processors, cause the one or more processors to perform the method of:

in an operating system environment controlled by a single operating system kernel instance, establishing a global zone and at least a first non-global zone for isolating processes in the first non-global zone from processes in other non-global zones;

receiving, from a first process executing in association with the first non-global zone, a first request to perform a first operation;

in response to the first request, determining whether performing the first operation enables the first process to obtain additional privileges for which the first process is not authorized; and

denying the first request if performing the first operation enables the first process to obtain additional privileges for which the first process is not authorized.

42. (New) The computer readable medium of claim 41, wherein each non-global zone has a set of allowable privileges for processes executing within the non-global zone.

43. (New) The computer readable medium of claim 42, wherein the first operation comprises obtaining control of a second process, wherein the first process has a first set of process privileges, wherein the second process has a second set of process privileges, and

wherein determining whether performing the first operation enables the first process to obtain additional privileges for which the first process is not authorized comprises:

determining if a zone identifier of the first process matches a zone identifier of the second process;

if the zone identifiers do not match:

determining if the first process is associated with a non-global zone; and if so, concluding that performing the first operation enables the first process to obtain additional privileges for which the first process is not authorized;

if the first process is not associated with a non-global zone, determining if the first process has a privilege to control processes in other zones; and if the first process does not have the privilege to control processes in other zones, concluding that performing the first operation enables the first process to obtain additional privileges for which the first process is not authorized;

determining if a user identifier of the first process matches a user identifier of the second process;

if the user identifiers do not match, determining if the first process has a privilege to take control of processes belonging to other user identifiers; and if the first process does not have the privilege to take control of processes belonging to other user identifiers, concluding that performing the first operation enables the first process to obtain additional privileges for which the first process is not authorized;

determining if the first set of process privileges includes every privilege in the second set of process privileges; and if the first set of process privileges does not include every privilege in the second set of process privileges, concluding that performing the first

operation enables the first process to obtain additional privileges for which the first process is not authorized.

44. (New) The computer readable medium of claim 43, wherein the first non-global zone has a first set of allowable privileges, and wherein the method further comprises:

determining if the user identifier of the second process is a privileged user identifier;

if the user identifier of the second process is not a privileged user identifier, concluding that performing the first operation does not enable the first process to obtain additional privileges for which the first process is not authorized; thus, the first request is granted;

if the user identifier of the second process is a privileged user identifier, determining if the first process is associated with the global zone;

if the first process is associated with the global zone, determining if the first process has all global zone privileges; and if not, concluding that performing the first operation enables the first process to obtain additional privileges for which the first process is not authorized;

if the first process is not associated with the global zone, determining if the first process has all of the privileges in the first set of allowable privileges; and if not, concluding that performing the first operation enables the first process to obtain additional privileges for which the first process is not authorized.

45. (New) The computer readable medium of claim 42, wherein establishing the first non-global zone for isolating processes in the first non-global zone from processes in other non-global zones, comprises:

setting a privilege limit for the first non-global zone, the privilege limit indicating the set of allowable privileges for processes executing within the first non-global zone.

46. (New) The computer readable medium of claim 45, wherein the privilege limit is represented as a bit mask passed to the first non-global zone when the first non-global zone is created, the method further comprising:

comparing privileges held by a process joining the first non-global zone against the bit mask; and

removing any privileges not in the bit mask from the process joining the first non-global zone.

47. (New) The computer readable medium of claim 41, wherein performing the first operation comprises accessing an object, the method further comprising:

determining whether the first process has permission to access the object.

48. (New) The computer readable medium of claim 41, wherein the first operation includes one of:

mounting/unmounting a file system, overriding file system permissions, binding to a privileged network port, and controlling other processes with different user identifiers.

49. (New) The computer readable medium of claim 42, wherein the first operation comprises changing a user identifier associated with the first process, wherein the first non-global zone has a first set of allowable privileges, and wherein determining whether performing the first operation enables the first process to obtain additional privileges for which the first process is not authorized comprises:

determining if the first operation is changing the user identifier associated with the first process to a privileged user identifier;

if the first operation is not changing the user identifier associated with the first process to a privileged user identifier, determining if the first process has a privilege to set its own user identifier; and if not, concluding that performing the first operation enables the first process to obtain additional privileges for which the first process is not authorized;

if the first operation is changing the user identifier associated with the first process to a privileged user identifier, determining whether the first process has all of the privileges in the first set of allowable privileges, and if not, concluding that performing the first operation enables the first process to obtain additional privileges for which the first process is not authorized.

50. (New) The computer readable medium of claim 41, wherein the method further comprises:

receiving, from a second process executing in association with the global zone, a second request to perform a second operation;

in response to the second request, determining whether performing the second operation enables the second process to obtain additional privileges for which the second process is not authorized; and

denying the second request if performing the second operation enables the second process to obtain additional privileges for which the second process is not authorized.

51. (New) The computer readable medium of claim 50, wherein the second operation comprises obtaining control of a third process, wherein the second process has a first set of

process privileges, wherein the third process has a second set of process privileges, and wherein determining whether performing the second operation enables the second process to obtain additional privileges for which the second process is not authorized comprises:

determining if a zone identifier of the second process matches a zone identifier of the third process;

if the zone identifiers do not match:

determining if the second process is associated with a non-global zone; and if so, concluding that performing the second operation enables the second process to obtain additional privileges for which the second process is not authorized;

if the second process is not associated with a non-global zone, determining if the second process has a privilege to control processes in other zones; and if the second process does not have the privilege to control processes in other zones, concluding that performing the second operation enables the second process to obtain additional privileges for which the second process is not authorized;

determining if a user identifier of the second process matches a user identifier of the third process;

if the user identifiers do not match, determining if the second process has a privilege to take control of processes belonging to other user identifiers; and if the second process does not have the privilege to take control of processes belonging to other user identifiers, concluding that performing the second operation enables the second process to obtain additional privileges for which the second process is not authorized;

determining if the first set of process privileges includes every privilege in the second set of process privileges; and if the first set of process privileges does not include every privilege in the second set of process privileges, concluding that performing the second

operation enables the second process to obtain additional privileges for which the second process is not authorized;

determining if the user identifier of the third process is a privileged user identifier;

if the user identifier of the third process is not a privileged user identifier, concluding that performing the second operation does not enable the second process to obtain additional privileges for which the second process is not authorized; thus, the second request is granted;

if the user identifier of the third process is a privileged user identifier, determining if the second process is associated with the global zone; and

if the second process is associated with the global zone, determining if the second process has all global zone privileges; and if not, concluding that performing the second operation enables the second process to obtain additional privileges for which the second process is not authorized.

52. (New) The computer readable medium of claim 50, wherein the second operation comprises changing a user identifier associated with the second process, and wherein determining whether performing the second operation enables the second process to obtain additional privileges for which the second process is not authorized comprises:

determining if the second operation is changing the user identifier associated with the second process to a privileged user identifier;

if the second operation is not changing the user identifier associated with the second process to a privileged user identifier, determining if the second process has a privilege to set its own user identifier; and if not, concluding that performing the second operation enables the

second process to obtain additional privileges for which the second process is not authorized;

if the second operation is changing the user identifier associated with the second process to a privileged user identifier, determining whether the second process has all global zone privileges, and if not, concluding that performing the second operation enables the second process to obtain additional privileges for which the second process is not authorized.

53. (New) The computer readable medium of claim 50, wherein the second operation includes one of:

modifying all process privileges, writing to system administration file, opening device holding kernel memory, modifying operating system code, accessing file systems restricted to root user, setting the system clock, changing scheduling priority of an executing process, reserving resources for an application, directly accessing a network layer and loading kernel modules.